

FortiAnalyzer

Zentralisiertes Logging, Reporting und Analyse

Mehr Transparenz und Planungssicherheit

Die FortiAnalyzer-Produktfamilie bietet Echtzeit-Netzwerk-Logging-, Analyse- und Reporting-Funktionen in Form einer Appliance, die auf Log-Daten von FORTINET-Geräten und auch von Produkten anderer Hersteller sicher zusammenführen. Sämtliche Informationen über Traffic, Events, Viren, Angriffe, Web-Inhalte und E-Mail-Daten können archiviert und kontrolliert werden. Eine umfassende Auswahl an Standardberichten gehört ebenso zum Lieferumfang wie die Möglichkeit, beliebige benutzerdefinierte Reports zu generieren. FortiAnalyzer bietet außerdem erweiterte Sicherheitsmanagement-Funktionen wie die Archivierung von Quarantäne-Dateien, Ereignis-Korrelation, Schwachstellen-Management, Traffic-Analyse und die Archivierung von E-Mail-, Webzugriffs-, Instant-Messaging- und Dateitransfer-Inhalten.

Informationen über alle Security-Events

Mit der FortiAnalyzer-Produktlinie ist es möglich, automatisiert jeden Zeitpunkt in der Event-Historie detailliert zu analysieren – ohne die Notwendigkeit manueller Suchen und Auswertungen. Event-Korrelationen verteilter Security-Ereignisse, auch über definierbare Zeiträume hinweg, erleichtern die forensische Analyse aller sicherheitsrelevanten Vorkommnisse ebenso wie das Auffinden von Schwachstellen in Unternehmens-Infrastrukturen.

Erweitertes Schwachstellen-Management

Ab dem FortiAnalyzer Release 4.0 ist es möglich, mit einem erweiterten Set von Signaturen die eigene Infrastruktur oder die von Kunden detailliert auf Schwachstellen zu untersuchen und gleichzeitig Reports über die notwendigen Korrektur- und/oder Update-Maßnahmen zu generieren.

Grafisches Reporting

Eine Vielzahl von voreingestellten grafischen Auswertungen sowie die Möglichkeit, kundenspezifische grafische Reports zu erstellen, erlauben einen detaillierten Überblick über alle Sicherheitsvorkommnisse und Langzeitanalysen.

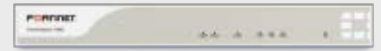
Granulare Informationen

Die FortiAnalyzer-Benutzeroberfläche gestattet die granulare Analyse einzelner Events in einer nahezu beliebigen Tiefe. So ist es leicht möglich, die Ereignisse im Unternehmensnetz zu deuten und die Quelle und Ursache von Unregelmäßigkeiten aufzuspüren.

Echtzeit-Analyse

Sämtliche Ereignisse können bis auf User-Ebene, Netzwerk-Segment oder Traffic-Verhalten in Echtzeit angezeigt und untersucht werden. So ist eine zeitnahe Reaktion auf etwaige Sicherheitsbedrohungen einfach möglich.

Datenblatt



FortiAnalyzer macht den Unterschied

Die FortiAnalyzer-Produktfamilie liefert den detaillierten Überblick über die gesamte Security-Infrastruktur – und das mit granularem grafischen Reporting. Der Umfang der Funktionen zum Sammeln und Auswerten von Daten deckt Sicherheitslücken auf und eliminiert Schwachstellen, bevor Daten ungewollt ausgespäht oder Sicherheitsmechanismen überwunden werden.

Die FortiAnalyzer Tools zur forensischen Analyse erlauben Auswertungen und Reports über Aktivitäten und Verhaltensmuster bis auf User-Ebene, während die Schwachstellen-Management-Engine Sicherheitslücken auf Endgeräte und Server aufdeckt, kategorisiert und Gegenmaßnahmen aufzeigt.

FortiAnalyzer-Appliances werden mit einem Jahr Hardware-Garantie und einem auf 90 Tage limitierten Software-Update-Service ausgeliefert.

Funktion	Vorteil
Netzwerk-Event Korrelation	Erlaubt zeitnahe Analyse von über das Netzwerk und verschiedene Komponenten verteilte Security-Ereignisse und entsprechende Reaktionen darauf.
Übersichtliche grafische Auswertungen & Reports	Ermöglicht das Netzwerk übergreifende Reporting von Events, Aktivitäten und Trends auf FortiGate- und 3rd-Party-Produkten.
Skalierbare Performance und Kapazität	Die für alle Unternehmen geeigneten Modelle bieten die jeweils optimale Unterstützung von bis zu mehreren 1000 FortiGates und 10000en von FortiClients.
Zentrales Logging unterschiedlicher Record Typen	Inklusive Traffic Activity, System Events, Viren, Angriffe, Web Filter und Messaging Activity/Data.
Nahtlose Integration in Fortinet-Produktline	Die optimale Anpassung an das gesamte Portfolio ermöglichen die Administration der FortiAnalyzer-Familie von einer FortiGate- oder einer FortiManager-Konsole.

Technische Spezifikationen	FAZ-100C	FAZ-400B	FAZ-1000C	FAZ-2000B	FAZ-4000A
Hardware-Spezifikationen					
10/100/1000 Schnittstellen (Kupfer, RJ-45)	2	1	4	6	2
10/100 Switch-Schnittstellen (Kupfer, RJ-45)	1	0	0	0	0
Anzahl Festplatten	1	1 / plus 1 opt.	1 / plus 3 opt.	2 / plus 4 opt.	12
Gesamt HD-Kapazität (standard/vollbestückt)	1 TB	0,5 / 1 TB	1 / 4 TB	2 / 6 TB	6 / 6 TB
RAID Management	Nein	Ja m. opt. 2. HD (0, 1)	Ja m. opt. 2. HD (0, 1, 10)	Ja (0, 1, 5, 10, 50)	Ja (0, 1, 5, 10, 50)
Anzahl Logs (RAID 0)	912.680.550	912.680.550	3.865.470.566	5.798.205.850	5.798.205.850
Redundante Stromversorgung	Nein	Nein	Nein	Ja	Ja
System-Performance					
Logs/Sekunde	200	500	1.000	3.000	5.000
Empfangsrate	800 kbps	2 Mbps	4 Mbps	12 Mbps	20 Mbps
Anzahl Network-Devices	100	200	2.000	2.000	2.000
Anzahl FortiClients	100	2.000	Unlimitiert	Unlimitiert	Unlimitiert
FortiGate-Unterstützung	Alle	Alle	Alle	Alle	Alle
FortiMail-Unterstützung	Alle	Alle	Alle	Alle	Alle
FortiClient-Unterstützung	Premium	Premium	Premium	Premium	Premium
FortiManager-Unterstützung	Alle	Alle	Alle	Alle	Alle
Syslog-Device-Unterstützung	Ja	Ja	Ja	Ja	Ja
Abmessungen					
Höhe	4,45 cm	4,45 cm	4,45 cm	8,9 cm	8,9 cm
Breite	38 cm	44 cm	44 cm	44 cm	44 cm
Länge	16 cm	36,8 cm	62,7 cm	68,1 cm	68,6 cm
Gewicht	1,8 kg	4,5 kg	15,9 kg	26,1 kg	30,8 kg
Montierbar in 19"-Racks	Ja	Ja	Ja	Ja	Ja
Umgebung/Anforderungen					
Wechselstromanforderung	100–240 VAC, 50–60 Hz				
Stromverbrauch (max.)	1,5 A	4 A	7 A	8 A	9 A
Betriebstemperatur	0–40 °C	0–40 °C	0–35 °C	0–40 °C	0–40 °C
Lagerungstemperatur	-25–70 °C	-25–70 °C	-25–70 °C	-25–70 °C	-25–70 °C
Luftfeuchtigkeit	5–95%	5–95%	5–95%	5–95%	5–95%
Compliance					
	FCC-Klasse A Abschnitt 15, UL/CUL, C Tick, VCCI				

FortiGuard® Security Subscription Services liefern dynamische, automatische Updates für die Fortinet-Produkte. Das Fortinet Global Security Research Team stellt diese Updates zur Verfügung, um stets den aktuellsten Schutz gegen intelligente und kombinierte Angriffe zu bieten. Die Subscriptions beinhalten AntiVirus, Intrusion Detection, Web Filtering, AntiSpam, Vulnerability and Compliance Management, Applikationskontrolle und Sicherheits-Services für Datenbanken.

FortiCare® Support Services bieten neben den FortiOS,- Firewall- und VPN-Funktions-Updates auch den globalen Support für alle Fortinet-Produkte und Services. FortiCare Support-Verträge bieten je nach Support Level Agreement (SLA) 8 x 5 Enhanced Support inklusive „return and repair“ Hardware-Austausch oder 24 x 7 Comprehensive Support mit erweitertem Hardware-Austausch. Weitere Optionen umfassen Premium Support, Premium RMA und Professional Services. Alle Hardware-Produkte beinhalten eine einjährige Hardware-Garantie und 90-tägige Software-Updates.



GLOBALER HAUPTSITZ
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel.: +1-408-235-7700
Fax: +1-408-235-7737
www.fortinet.com/sales

FORTINET GERMANY
Wöhlerstraße 5
D-60323 Frankfurt am Main
Tel.: +49-69 710 423 535
Fax: +49 69 710 423 200
www.fortinet.de/sales



© 2010 Fortinet, Inc. Alle Rechte vorbehalten. Fortinet®, FortiGate® und FortiGuard® sind registrierte Marken der Fortinet, Inc., andere hierin erwähnte Fortinet-Namen können ebenfalls Marken von Fortinet sein. Alle anderen erwähnten Produkt- oder Unternehmensnamen sind Marken ihrer jeweiligen Eigner. Hierin enthaltene Leistungsmetriken wurden bei Labortests unter Idealbedingungen erreicht. Netzwerkvariablen, unterschiedliche Netzwerkbedingungen und andere Umstände können die Leistungsergebnisse beeinträchtigen. Fortinet lehnt jegliche Gewährleistungen ab, ob ausdrücklich oder stillschweigend, mit Ausnahme des Falles, dass Fortinet einen rechtswirksamen Vertrag mit einem Käufer eingeht, in dem ausdrücklich gewährleistet wird, dass die Leistung des bestimmten Produkts den hierin enthaltenen Leistungsmetriken entsprechen wird. Im Sinne absoluter Klarheit wird festgestellt, dass eine solche Gewährleistung darauf beschränkt bleibt, dass die Leistung nur bei denselben Idealbedingungen wie in den Labortests von Fortinet erreicht wird. Fortinet lehnt in vollem Umfang jegliche Garantien ab. Fortinet behält sich das Recht vor, diese Publikation ohne vorherige Ankündigung zu ändern, anzupassen, zu übertragen oder anderweitig zu überarbeiten, und es findet die jeweils aktuellste Version Anwendung. Bestimmte Fortinet-Produkte sind lizenziert unter der US-Patent-Nr. 5,623,600. FG-80CM-DAT-R1-0209